



PATENT ABSTRACTS OF JAPAN

(11) Publication number: 11004407 A

(43) Date of publication of application: 06.01.99

(51) Int. Cl.

H04N 5/91

H04H 1/00

H04L 9/08

H04N 7/167

(21) Application number: 09156312

(22) Date of filing: 13.06.97

(71) Applicant: MATSUSHITA ELECTRIC IND CO LTD

(72) Inventor: MAEDA TAKIO

(54) BROADCAST SIGNAL RECORDING AND REPRODUCING DEVICE

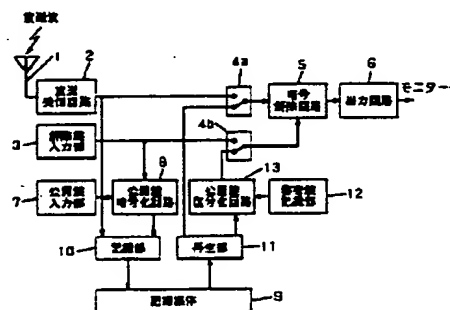
(57) Abstract:

PROBLEM TO BE SOLVED: To provide a device by which only an imposed viewer reproduces a broadcast signal by entering a decode key to decode an enciphered broadcast signal, enciphering the key with a public key enciphering means, recording the broadcast signal enciphered by the public key enciphering means based on the broadcast signal onto a recording medium, decoding the enciphered broadcast signal with a decoding key decoded by the private key, reproducing and outputting the decoded signal.

SOLUTION: A received broadcast signal is recorded on a recording medium 9. A viewer uses a decoding key input section 3 to acquire a decoding key. A public key enciphering circuit 8 enciphers the acquired decoding key with the public key entered by a public key entry section 7 to record the decoding key on a recording medium 9 via a recording section 10. A reproduction section 11 reads the recording medium 9, outputs a broadcast signal to an encryption decoding circuit 5, and the enciphered decoding key is outputted to a public key decoding circuit 13. The public key decoding circuit 13 decodes the private key stored in a private key

storage section 12, by using the enciphered decoding key at the public key decoding circuit 13 to output the decoded key to an encryption decoding circuit 5. It is decoded and outputted on a monitor.

COPYRIGHT: (C)1999,JPO



(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平11-4407

(43)公開日 平成11年(1999)1月6日

(51)IntCl⁶

識別記号

FI

H04N 5/91

H04N 5/91

P

H04H 1/00

H04H 1/00

F

H04L 9/08

H04L 9/00

601A

H04N 7/167

601E

H04N 7/167

Z

審査請求 未請求 請求項の数3 OL (全7頁)

(21)出願番号

特願平9-156312

(22)出願日

平成9年(1997)6月13日

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 前田 多吉生

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

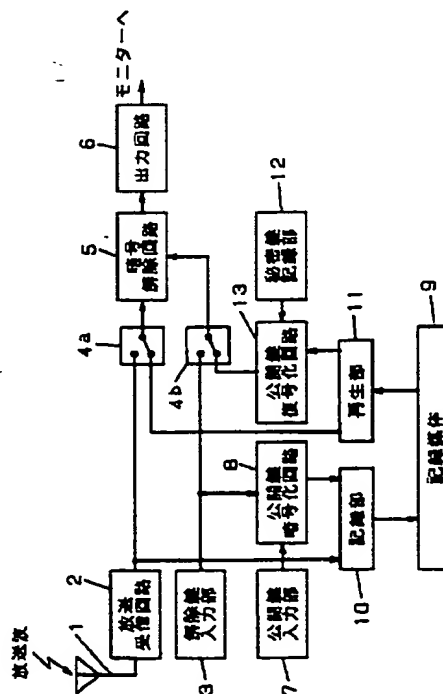
(74)代理人 弁理士 滝本 智之 (外1名)

(54)【発明の名称】 放送信号記録再生装置

(57)【要約】

【課題】 記録媒体が装置から分離可能であるとき、放送番組の著作権を保護しつつ、課金された視聴者のみが再生する機器を選択し、放送を再生することができない。

【解決手段】 暗号化された放送信号を受信する受信手段1と、前記放送信号の暗号化を解除する解除鍵を入力する解除鍵入力手段3と、前記解除鍵入力手段より入力された解除鍵を公開鍵暗号系の公開鍵により暗号化する公開鍵暗号化手段8と、前記放送信号と暗号化後の解除鍵を記録媒体に記録する記録手段9と、暗号化後に記録された前記解除鍵を前記公開鍵と対応する秘密鍵を用いて復号化する公開鍵復号化手段13と、復号化された前記解除鍵により記録された前記放送信号の暗号化を解除する暗号解除手段5を備える。



【特許請求の範囲】

【請求項 1】 暗号化された放送信号を受信する受信手段と、前記放送信号の暗号化を解除する解除鍵を入力する解除鍵入力手段と、前記解除鍵入力手段より入力された解除鍵を公開鍵暗号系の公開鍵により暗号化する公開鍵暗号化手段と、前記放送信号と前記公開鍵暗号化手段により暗号化された解除鍵を記録媒体に記録する記録手段と、前記記録媒体に記録された解除鍵を前記公開鍵と対応する秘密鍵を用いて復号化する公開鍵復号化手段と、復号化された解除鍵により記録された前記放送信号の暗号化を解除する暗号解除手段と、前記暗号化手段により暗号化を解除された放送信号を再生し、出力する再生・出力手段とを備えたことを特徴とする放送信号記録再生装置。

【請求項 2】 公開鍵暗号化手段が複数の公開鍵を入力し、暗号化された解除鍵を複数生成する公開鍵暗号化手段であり、記録された複数の暗号化後の解除鍵の中から一つの公開鍵に対応する暗号化された解除鍵を選択し、前記公開鍵復号化手段に出力する選択手段を備えたことを特徴とする請求項 1 記載の放送信号記録再生装置。

【請求項 3】 第 1 の公開鍵によって暗号化された解除鍵を前記第 1 の公開鍵に対応する第 1 の秘密鍵を用いて復号化する第 1 の公開鍵復号化手段と、前記第 1 の公開鍵復号化手段により復号化された解除鍵を前記第 1 の公開鍵とは別の第 2 の公開鍵により暗号化する公開鍵暗号化手段と、前記第 2 の公開鍵に対応する第 2 の秘密鍵により前記公開鍵暗号化手段により暗号化された解除鍵を復号化する第 2 の公開鍵復号化手段とを備えたことを特徴とする請求項 1 記載の放送信号記録再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、放送信号を記録媒体に記録し、再生することのできる放送信号記録再生装置に関するものである。

【0002】

【従来の発明】従来より、有料システムとするために放送信号を暗号化して、著作権を保護しているCATVや衛星放送などがある。配信された放送信号を著作権を保護しつつ記録媒体に記録するための装置として、「特開平 7-154385 号公報：妨害重畳情報処理装置」等が開示されている。

【0003】以下、著作権を保護する機能を有する妨害重畳情報処理装置の構成と動作を、図 5 を用いて同時に説明する。

【0004】図 5 に示すように、放送信号の受信手段である放送受信回路 502 はアンテナ 501 を介して放送信号を受信する。得られた放送信号は、暗号化された信号であり、この暗号化された受信信号がそのまま再生される場合は、切換回路 503a を経て暗号解除回路 504 に送られる。解除鍵入力部 505 は前記暗号化された

放送信号の暗号化を解除するための解除鍵を視聴者の入力、あるいは電話等の通信手段を用いて取得する。前記解除鍵入力部 505 により取得された解除鍵はスイッチ 503b を経て前記暗号解除回路 504 に送られ、前記暗号解除回路 504 は暗号化された前記放送信号の暗号を解除し、出力回路 506 を通じてモニタに送り、再生する。この暗号化された受信信号が記録される場合は、記録部 507 に送られ、同時に解除鍵入力部 505 により取得した解除鍵も記録部 507 に送られ、記録媒体 508 に記録される。記録された放送信号と解除鍵は再生部 509 によりそれぞれ切換回路 503a、切換回路 503b を介して暗号解除回路 504 に送られる。暗号解除回路 504 は暗号化された前記放送信号の暗号を解除し、出力回路 506 を通じてモニタに送り、放送を再生する。

【0005】なお、放送局毎、放送チャンネル毎に異なる暗号化が行われている。したがって、放送局や放送チャンネル固有の解除鍵データにより解除しない限り、視聴可能な状態には再生されない。即ち、これにより、放送信号を記録できても、専用の妨害重畳情報処理装置がない限り再生ができないため、著作権の保護が可能となる。

【0006】

【発明が解決しようとする課題】しかしながら、上記のような従来の装置では、記録媒体が入れ替え可能であるなら、記録媒体に記録された放送信号は同じ種類の専用の処理装置であればどれでも再生が可能である。

【0007】即ち、従来の装置を用いた有料放送システムでは、もし記録媒体が装置から取り外し可能であれば、記録媒体を盗金されていない装置に接続することにより、その装置でも再生が可能となり、著作権を保護できない。したがって、著作権を保護するためには、記録媒体が装置から分離できない形の装置を用いるしか有料放送システムを構築できなかった。

【0008】本発明は、従来の放送信号記録再生装置のこのような課題を考慮し、放送信号を記録した記録媒体が装置から分離可能であり、有料放送システムにおいて盗金された視聴者のみが記録媒体に記録された放送信号を再生できる放送信号記録再生装置を提供することを目的とする。

【0009】

【課題を解決するための手段】請求項 1 記載の本発明は、暗号化された放送信号を受信する受信手段と、前記放送信号の暗号化を解除する解除鍵を入力する解除鍵入力手段と、前記解除鍵入力手段より入力された解除鍵を公開鍵暗号系の公開鍵により暗号化する公開鍵暗号化手段と、前記放送信号と前記公開鍵暗号化手段により暗号化された解除鍵を記録媒体に記録する記録手段と、前記記録媒体に記録された解除鍵を前記公開鍵と対応する秘密鍵を用いて復号化する公開鍵復号化手段と、復号化さ

れた解除鍵により記録された前記放送信号の暗号化を解除する暗号解除手段と、前記暗号化手段により暗号化を解除された放送信号を再生し、出力する再生・出力手段とを備えたことを特徴とする放送信号記録再生装置である。

【0010】請求項2記載の本発明は、前記公開鍵暗号化手段が複数の公開鍵を入力し、暗号化された解除鍵を複数生成する公開鍵暗号化手段であり、記録された複数の暗号化後の解除鍵の中から一つの公開鍵に対応する暗号化された解除鍵を選択し、前記公開鍵復号化手段に出力する選択手段を備えたことを特徴とする請求項1記載の放送信号記録再生装置である。

【0011】請求項3記載の本発明は、第1の公開鍵によって暗号化された解除鍵を前記第1の公開鍵に対応する第1の秘密鍵を用いて復号化する第1の公開鍵復号化手段と、前記第1の公開鍵復号化手段により復号化された解除鍵を前記第1の公開鍵とは別の第2の公開鍵により暗号化する公開鍵暗号化手段と、前記第2の公開鍵に対応する第2の秘密鍵により前記公開鍵暗号化手段により暗号化された解除鍵を復号化する第2の公開鍵復号化手段とを備えたことを特徴とする請求項1記載の放送信号記録再生装置である。

【0012】請求項1記載の放送信号記録再生手段は、受信手段が暗号化された放送信号を受信し、解除鍵入力手段が前記放送信号の暗号化を解除する解除鍵を入力し、公開鍵暗号化手段が解除鍵を公開鍵暗号系の公開鍵により暗号化し、記録手段が前記放送信号と暗号化後の解除鍵を記録媒体に記録し、公開鍵復号化手段が記録された暗号化後の前記解除鍵を前記公開鍵と対応する秘密鍵を用いて復号化し、暗号解除手段が記録された前記放送信号の暗号化を解除鍵を用いて解除し、再生・出力手段が暗号解除された放送信号を再生し、出力する。

【0013】請求項2記載の放送信号記録再生手段では、前記公開鍵暗号化手段が複数の公開鍵を入力し、暗号化された解除鍵を複数生成し、選択手段が記録手段に記録された複数の暗号化後の解除鍵の中から一つの公開鍵に対応する暗号化された解除鍵を選択し、前記公開鍵復号化手段に出力する。

【0014】請求項3記載の放送信号記録再生手段では、公開鍵暗号化手段が前記公開鍵復号手段により復号化された解除鍵を前記公開鍵とは別の公開鍵により再度暗号化し、公開鍵復号化手段が前記別の公開鍵に対応した秘密鍵により前記再度暗号化された解除鍵を再度復号化し前記暗号解除手段に出力する。

【0015】

【発明の実施の形態】以下、本発明の実施の形態について、図面を用いて説明する。

【0016】(実施の形態1) 図1は、本発明の請求項1記載の実施の形態の放送信号記録再生装置の構成図であり、同図を参照しながら、本実施の形態の構成を説明

する。

【0017】図1において、本発明の受信手段としての放送受信回路2は、アンテナ1から得られた放送信号を受信し、放送信号を出力する回路手段である。解除鍵入力部3は前記放送信号の暗号を解除する解除鍵を電話等の通信手段を用いて取得するものである。切換回路4a、切換回路4bはそれぞれ入力データの流れを切り換える回路である。暗号解除回路5は暗号化された放送信号と解除鍵を入力し、復号化した放送信号を出力する回路である。出力回路6は暗号解除回路5からの出力を得てモニタ(図示省略)へ再生信号として出力する手段である。公開鍵入力部7は公開鍵暗号系の公開鍵を入力する手段である。

【0018】公開鍵暗号化回路8は解除鍵入力部3から解除鍵を入力し、公開鍵入力部7により入力された公開鍵で暗号化する回路である。記録媒体9はデータを記録する手段であり、取りはずすことも可能である。記録部10は入力されたデータを記録媒体9に記録する。再生部11は記録媒体9に記録されたデータを読み取る。公開鍵暗号系の公開鍵とその公開鍵に対応する秘密鍵が本発明の放送信号記録再生装置に事前に割り当てられており、秘密鍵記録部12は機器固有の秘密鍵を保持する手段である。公開鍵復号化回路13は再生部11から出力されたデータを入力し、秘密鍵記録部12の鍵を用いて暗号化された解除鍵を復号化する手段である。

【0019】以上のような構成において、図1を参照しながら、本実施例の動作を説明する。まず、リアルタイムで、放送番組を視聴する場合について述べる。

【0020】図1に示すように、アンテナ1を介して、放送受信回路2により受信された放送信号は、切換回路4aを介して、暗号解除回路5に送られる。放送の視聴を希望する視聴者は解除鍵入力部3により解除鍵を取得し、切換回路4bを介して暗号解除回路5に送る。暗号解除回路5は入力された解除鍵を用いて入力された放送信号の暗号を解除し、出力回路6へ出力する。出力回路6は暗号の解除された放送信号をモニタへ出力する。これにより、視聴を希望する視聴者だけが放送を見ることができる。

【0021】次に、番組を記録し、それを再生する場合について述べる。

(ステップ101) アンテナ1を介して放送受信回路2により受信された放送信号は記録部10を介して記録媒体9に記録される。

(ステップ102) 放送の視聴を希望する視聴者は解除鍵入力部3により解除鍵を取得する。

(ステップ103) 公開鍵入力部7により、視聴者は公開鍵を入力する。このとき、視聴者は記録する放送信号を再生する機器に割り当てられた公開鍵を入力する。即ち、記録する機器と同じ機器で再生する場合は、その機器固有の公開鍵を入力し、記録する機器と再生する機

器が別々の場合は再生する機器固有の公開鍵を入力する。

【0022】(ステップ104) 公開鍵暗号化回路8は解除鍵入力部3により取得された解除鍵を公開鍵入力部7で入力された公開鍵を用いて暗号化し、記録部10を介して記録媒体9に記録する。

(ステップ105) 再生部11は記録媒体9を読み取り、放送信号を切換回路4aを介して暗号解除回路5へ出力する。

(ステップ106) 再生部11は暗号化後の解除鍵を公開鍵復号化回路13に出力する。

(ステップ107) 公開鍵復号化回路13は入力された暗号化後の前記解除鍵を秘密鍵記録部12に保持されている秘密鍵を用いて復号化し、復号化した解除鍵を切換回路4bを介して暗号解除回路5に出力する。このとき、前記秘密鍵が解除鍵の暗号化に用いられた公開鍵に対応しなければ、元の解除鍵に復号することはできない。

(ステップ108) 暗号解除回路5は入力された放送信号を入力された解除鍵を用いて復号化し、出力回路6を介してモニタに出力する。

【0023】以上のことから、放送信号の解除鍵は、視聴者が選択した機器固有の公開鍵を用いて暗号化した後に記録媒体に記録されるため、その公開鍵と対応する秘密鍵を有する機器のみが解除鍵を復号化でき、放送信号の再生が可能となる。

【0024】(実施の形態2) 図2は、本発明の請求項2記載の実施の形態例の放送信号記録再生装置の構成図であり、図3はデータ構成を説明する図であり、同図を参照しながら、本実施の形態の構成を説明する。

【0025】図2において、公開鍵リスト入力部21は複数の公開鍵を取得し、記録する手段である。公開鍵記録部22は機器固有の秘密鍵に対応する公開鍵を保持する手段である。暗号リスト選択部23は再生部11から複数の暗号化された解除鍵リストを入力し、前記公開鍵記録部22を索引として一つの解除鍵データを選択する手段である。前記以外の構成は実施例1と同じである。以上のような構成において、図2と図3を参照しながら、本実施例の動作を説明する。リアルタイムで、放送番組を視聴する場合は実施例1と同じである。

【0026】次に、番組を記録し、それを再生する場合について述べる。

(ステップ201) 実施例1の(ステップ101)と同じ。

(ステップ202) 実施例1の(ステップ102)と同じ。

(ステップ203) 公開鍵リスト入力部21により、視聴者は記録する放送信号を再生する可能性の有る機器に割り当てられた複数の公開鍵を入力する。

(ステップ204) 公開鍵暗号化回路8は解除鍵入力

部3により取得された解除鍵を公開鍵リスト入力部21で入力された公開鍵を用いてそれぞれ暗号化し、暗号化した複数の解除鍵を記録部10を介して記録媒体9に記録する。図3のデータ構成を用いて説明すると、(ステップ203)において、公開鍵31a、公開鍵31b、公開鍵31cが視聴者により入力された公開鍵であるとする、それらにより暗号化された解除鍵はそれぞれ暗号化解除鍵データ32a、暗号化解除鍵データ32b、暗号化解除鍵データ32cとなり、この公開鍵31a、公開鍵31b、公開鍵31c、暗号化解除鍵データ32a、暗号化解除鍵データ32b、暗号化解除鍵データ32cが記録媒体9に記録される。

【0027】(ステップ205) 実施例1の(ステップ105)と同じ。

(ステップ206) 再生部11は(ステップ204)で記録されたデータリストを暗号リスト選択部23に出力する。

(ステップ207) 暗号リスト選択部23は複数の暗号化された解除鍵と、公開鍵記録部22に保持されている公開鍵を用いて、対応する暗号化解除鍵を選択する。図3のデータ構成を用いて説明すると、公開鍵31a、公開鍵31b、公開鍵31cと公開鍵記録部22に記録された公開鍵を比較し、同じ公開鍵に対応した暗号化解除鍵を選択し、公開鍵復号化回路13に出力する。

(ステップ208) 実施例1の(ステップ107)と同じ。

(ステップ209) 実施例1の(ステップ108)と同じ。

【0028】以上のことから、放送信号の解除鍵は、視聴者を選択した複数の機器固有の公開鍵を用いて暗号化した後に記録媒体に記録されるため、その複数の公開鍵の中のどれかと対応する秘密鍵を有する機器でのみ再生が可能となる。

【0029】(実施の形態3) 図4は、本発明の請求項3記載の実施の形態の放送信号記録再生装置の構成図であり、同図を参照しながら、本実施の形態の構成を説明する。

【0030】図4において、認証部41は公開鍵記録部42、公開鍵記録部43が保持している公開鍵に対応する秘密鍵を保持する秘密鍵記録部43、公開鍵復号化回路44、公開鍵暗号化回路45を備えており、本実施例の放送記録再生装置から分離することが可能である。公開鍵記録部22は(実施例2)と同様に機器固有の公開鍵と秘密鍵を保持する手段である。その他の構成は(実施例1)と同様である。以上のような構成において、図4を参照しながら、本実施例の動作を説明する。リアルタイムで、放送番組を視聴する場合は実施例1と同じである。

【0031】次に、番組を記録し、それを再生する場合について述べる。

(ステップ301) 実施例1の(ステップ101)と同じ。

(ステップ302) 実施例1の(ステップ102)と同じ。

(ステップ303) 認証部41が本実施例の放送記録再生装置に接続されている場合は、公開鍵記録部42の公開鍵を公開鍵暗号化回路8に出力する。認証部41が接続されていない場合は、公開鍵暗号化回路8は有効な公開鍵を受け取ることはできない。

【0032】(ステップ304) 実施例1の(ステップ104)と同じ。

(ステップ305) 実施例1の(ステップ105)と同じ。

(ステップ306) 再生部11は暗号化後の解除鍵を公開鍵復号化回路44に出力する。

(ステップ307) 公開鍵復号化回路44は入力された解除鍵を秘密鍵記録部43の保持する秘密鍵を用いて復号化し、公開鍵暗号化回路45に出力する。

【0033】(ステップ308) 公開鍵暗号化回路45は入力した解除鍵を公開鍵記録部22の保持する公開鍵で再度暗号化し、公開鍵復号化回路13に出力する。

(ステップ309) 実施例1の(ステップ107)と同じ。

(ステップ310) 実施例1の(ステップ108)と同じ。

【0034】以上のことから、放送信号の解除鍵は、視聴者が有する認証部に保持される公開鍵により暗号化されたのち記録され、記録された解除鍵を復号化するにはその認証部が接続された機器のみが放送信号を再生することが可能となる。

【0035】

【発明の効果】以上のように本発明によれば、記録媒体が装置から分離可能であっても、有料放送システムにおいて課金された視聴者のみが記録媒体に記録された放送信号を再生できるという長所を有する。

【図面の簡単な説明】

【図1】本発明の実施の形態1の形態による放送信号記録再生装置の構成図

【図2】本発明の実施の形態2の形態による放送信号記録再生装置の構成図

【図3】本発明の実施の形態3の記録媒体に記録される暗号化解除鍵リストのデータ構成を模式的に示した図

【図4】本発明の実施の形態3による放送信号記録再生装置の構成を示す図

【図5】従来の情報処理装置の構成を示す図

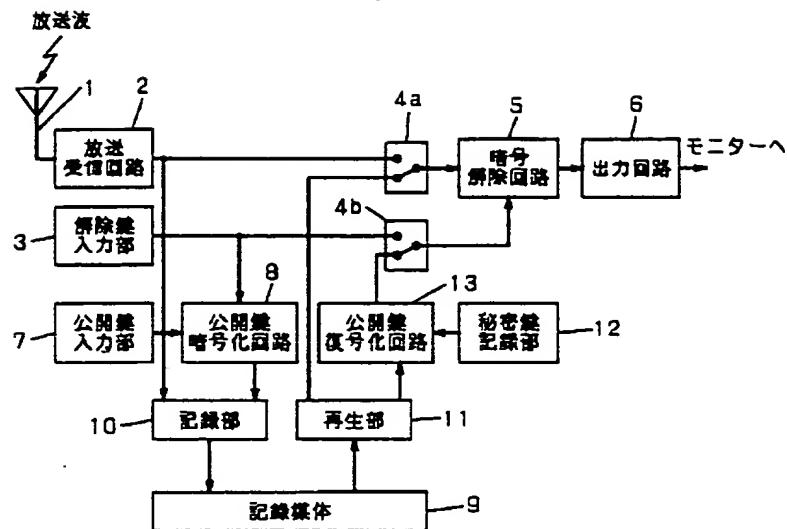
【符号の説明】

- 1 放送受信回路
- 2 解除鍵入力部
- 4 a 切換回路
- 4 b 切換回路
- 5 暗号解除回路
- 6 出力回路
- 7 公開鍵入力部
- 8 公開鍵暗号化回路
- 9 記録媒体
- 10 記録部
- 11 再生部
- 12 秘密鍵記録部
- 13 公開鍵復号化回路
- 21 公開鍵リスト入力部
- 22 公開鍵記録部
- 23 暗号リスト選択部
- 31 a 公開鍵A
- 31 b 公開鍵B
- 31 c 公開鍵C
- 32 a 暗号化解除鍵A
- 31 b 暗号化解除鍵B
- 31 c 暗号化解除鍵C
- 41 認証部

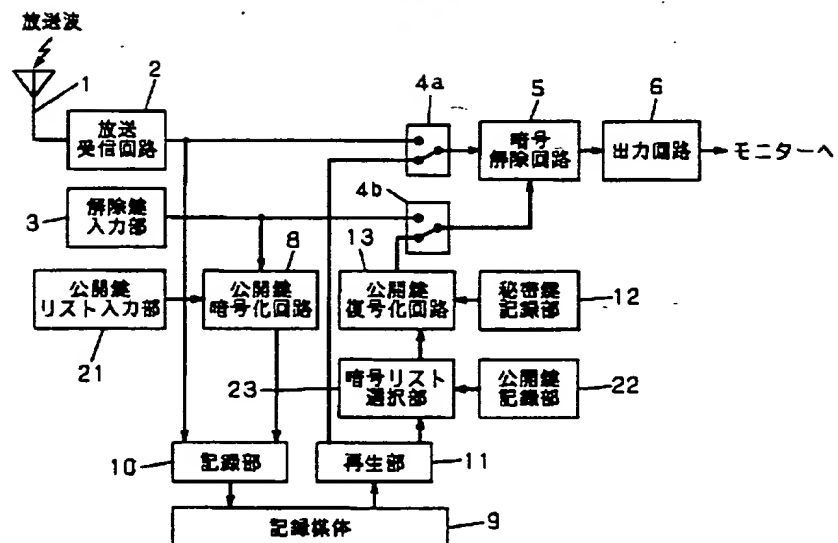
【図3】

31 a	開放鍵A	暗号化解除鍵A	32 a
31 b	開放鍵B	暗号化解除鍵B	32 b
31 c	開放鍵C	暗号化解除鍵C	32 c

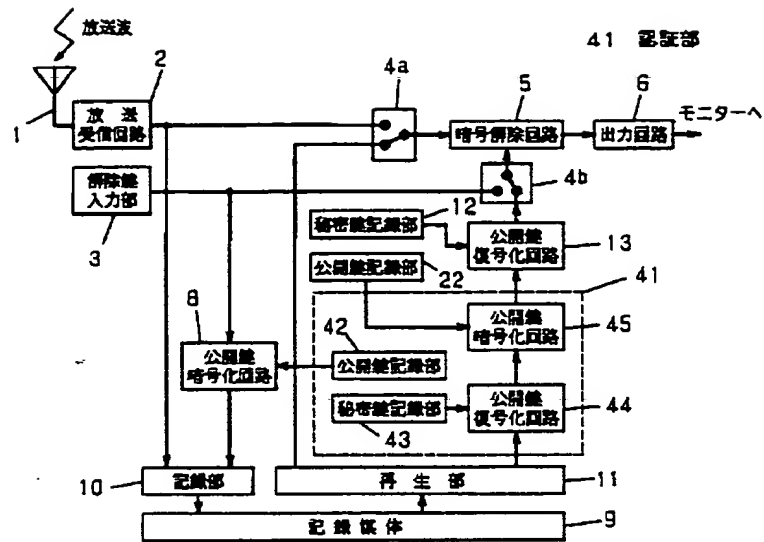
【図1】



【図2】



【図4】



【図5】

